PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-259108
(43)Date of publication of application : 13.09.2002

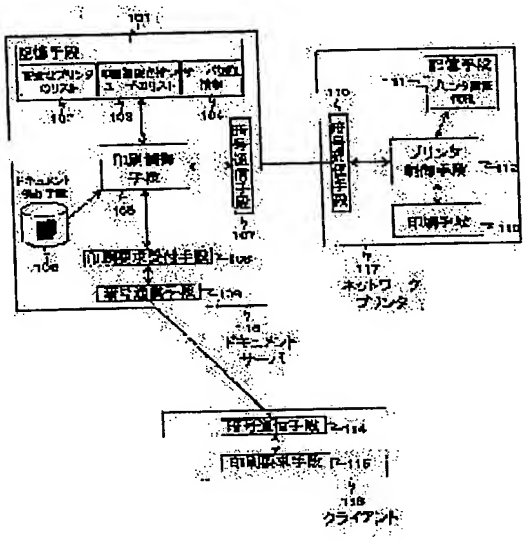
(51)Int.CI. G06F 3/12
B41J 29/00
B41J 29/38
G06F 15/00
H04L 9/32

(21)Application number : 2001-059015
(22)Date of filing : 02.03.2001

(71)Applicant : CANON INC
(72)Inventor : HISAMOTO SHINJI
KATO EIJI

(54) PRINTING SYSTEM, PRINTER, PRINTING METHOD, RECORDING MEDIUM, AND PROGRAM

(57)Abstract:
PROBLEM TO BE SOLVED: To prevent an illegal printer from pretending as a legal printer and to print out data only from a safe printer.
SOLUTION: The printing system constituted of a document server, a printer and a user client which are connected through a network stores a disclosed key certificate and a secret key corresponding to the certificate and executes printer certification on the basis of the certification in accordance with a request from the document server or the user client.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁(JP)

(12)公開特許公報（A）

(11)特許出願公開番号

特開２００２－２５９１０８

（Ｐ２００２－２５９１０８Ａ）

(43)公開日　平成14年9月13日(2002.9.13)

(51)Int.Cl.⁷		識別記号	FI			テーマコード(参考)
Ｇ０６Ｆ	3/12		Ｇ０６Ｆ	3/12	Ｋ	2C061
Ｂ４１Ｊ	29/00		Ｂ４１Ｊ	29/38	Ｚ	5B021
	29/38		Ｇ０６Ｆ	15/00 ３３０	Ｃ	5B085
Ｇ０６Ｆ	15/00	３３０	Ｂ４１Ｊ	29/00	Ｚ	5J104
Ｈ０４Ｌ	9/32		Ｈ０４Ｌ	9/00 ６７３	Ａ	

審査請求　未請求　請求項の数２１　ＯＬ　（全１９頁）

(21)出願番号　特願2001-59015(P2001-59015)

(22)出願日　平成13年3月2日(2001.3.2)

(71)出願人　000001007
キヤノン株式会社
東京都大田区下丸子3丁目30番2号

(72)発明者　久本　慎二
東京都大田区下丸子3丁目30番2号　キヤノン株式会社内

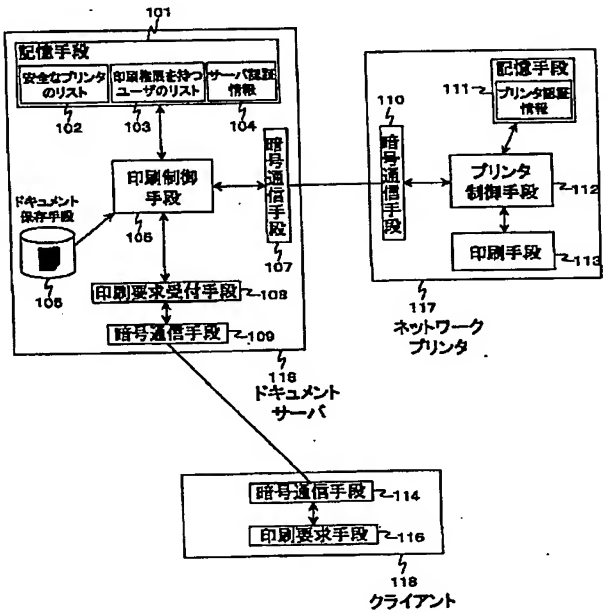
(72)発明者　加藤　英二
東京都大田区下丸子3丁目30番2号　キヤノン株式会社内

(74)代理人　100090273
弁理士　國分　孝悦

最終頁に続く

(54)【発明の名称】印刷システム、印刷装置、印刷方法、記録媒体及びプログラム

(57)【要約】
【課題】　プリンタのなりすましを防止し、安全なプリンタへのみ印刷することを課題とする。
【解決手段】　本発明の印刷システムは、ネットワークで接続されたドキュメンドサーバ、プリンタ、ユーザクライアントから構成される印刷システムであって、プリンタは公開鍵証明書とこれに対応する秘密鍵とを保有し、ドキュメントサーバもしくはユーザクライアントからの要求に応じて公開鍵証明書に基づくプリンタ認証を行う。



【特許請求の範囲】

【請求項１】　ネットワークで接続されたドキュメントサーバ、プリンタ、ユーザクライアントから構成される印刷システムであって、
プリンタは公開鍵証明書とこれに対応する秘密鍵とを保有し、ドキュメントサーバもしくはユーザクライアントからの要求に応じて公開鍵証明書に基づくプリンタ認証を行うことを特徴とする印刷システム。

【請求項２】　前記ドキュメントサーバは内蔵する機密情報と対応づけられた印刷許可プリンタのリストを保有し、印刷要求が行われた際に出力先のプリンタが前記許可プリンタのリストに含まれるかどうかに応じて前記出力先のプリンタに印刷データを送信することを特徴とする請求項１に記載の印刷システム。

【請求項３】　前記プリンタの公開鍵証明書は、前記プリンタの安全性を示す情報を含み、前記ドキュメントサーバは内蔵する機密情報と対応づけられた印刷許可プリンタの安全性を示す情報のリストを保有することを特徴とし、印刷要求が行われた際に出力先のプリンタの公開鍵証明書による認証を行い、前記プリンタが前記ドキュメントサーバの保有する許可プリンタの安全性を示す情報のリストに記された条件を満足するかどうかに応じて、前記出力先のプリンタに印刷データを送信することを特徴とする請求項１に記載の印刷システム。

【請求項４】　公開鍵証明書とこれに対応する秘密鍵とを保有し、外部からの要求に応じて公開鍵証明書に基づくプリンタ認証を行うことを特徴とする印刷装置。

【請求項５】　内蔵する機密情報と対応づけられた印刷許可プリンタのリストを保有し、印刷要求が行われた際に出力先のプリンタが前記印刷許可プリンタのリストに含まれるかどうかに応じてドキュメントサーバから送信された印刷データの印刷を行うことを特徴とする印刷装置。

【請求項６】　公開鍵証明書とこれに対応する秘密鍵とを保有し、外部からの要求に応じて公開鍵証明書に基づくプリンタ認証を行うステップを有することを特徴とする印刷方法。

【請求項７】　内蔵する機密情報と対応づけられた印刷許可プリンタのリストを保有し、印刷要求が行われた際に出力先のプリンタが前記印刷許可プリンタのリストに含まれるかどうかに応じて、前記出力先のプリンタに印刷データを送信するステップを有することを特徴とする印刷方法。

【請求項８】　公開鍵証明書とこれに対応する秘密鍵とを保有し、外部からの要求に応じて公開鍵証明書に基づくプリンタ認証を行う手順をコンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項９】　内蔵する機密情報と対応づけられた印刷許可プリンタのリストを保有し、印刷要求が行われた際に出力先のプリンタが前記印刷許可プリンタのリストに含まれるかどうかに応じて、前記出力先のプリンタに印刷データを送信する手順をコンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項１０】　公開鍵証明書とこれに対応する秘密鍵とを保有し、外部からの要求に応じて公開鍵証明書に基づくプリンタ認証を行う手順をコンピュータに実行させるためのプログラム。

【請求項１１】　内蔵する機密情報と対応づけられた印刷許可プリンタのリストを保有し、印刷要求が行われた際に出力先のプリンタが前記印刷許可プリンタのリストに含まれるかどうかに応じて、前記出力先のプリンタに印刷データを送信する手順をコンピュータに実行させるためのプログラム。

【請求項１２】　ネットワークで接続されたドキュメントサーバ、プリンタ、ユーザクライアントから構成され、前記プリンタを経由する参照印刷を行う印刷システムであって、
印刷を行う機密情報の印刷権限を確認するため使用される印刷要求データの少なくとも一部を、前記ドキュメントサーバでのみ復号可能なように前記ユーザクライアントにおいて暗号化し送付することを特徴とする印刷システム。

【請求項１３】　前記ドキュメントサーバにおけるユーザ認証方式がユーザの公開鍵証明書に基づく認証であって、ユーザの公開鍵証明書にはユーザのアクセス権を示すクラス名が記載されており、前記ドキュメントサーバにおける印刷権限の確認がこのユーザの公開鍵証明書に記載されているクラス名に基づいて行われることを特徴とする請求項１２に記載の印刷システム。

【請求項１４】　印刷を行う機密情報の印刷権限を確認するため使用される印刷要求データの少なくとも一部を、ドキュメントサーバでのみ復号可能なように暗号化しプリンタ経由で前記ドキュメントサーバに送信することを特徴とする印刷装置。

【請求項１５】　プリンタ経由でユーザから印刷要求データを受信する受信手段と、
前記印刷要求データに基づくユーザ認証方式がユーザの公開鍵証明書に基づく認証であって、ユーザの公開鍵証明書にはユーザのアクセス権を示すクラス名が記載されており、ドキュメントサーバにおける印刷権限の確認がこのユーザの公開鍵証明書に記載されているクラス名に基づいて行う認証手段とを有することを特徴とする印刷装置。

【請求項１６】　印刷を行う機密情報の印刷権限を確認するため使用される印刷要求データの少なくとも一部を、ドキュメントサーバでのみ復号可能なように暗号化しプリンタ経由で前記ドキュメントサーバに送信するステップを有することを特徴とする印刷方法。

【請求項１７】　プリンタ経由でユーザから印刷要求データを受信する受信ステップと、
前記印刷要求データに基づくユーザ認証方式がユーザの公開鍵証明書に基づく認証であって、ユーザの公開鍵証明書にはユーザのアクセス権を示すクラス名が記載されており、ドキュメントサーバにおける印刷権限の確認がこのユーザの公開鍵証明書に記載されているクラス名に基づいて行う認証ステップとを有することを特徴とする印刷方法。
【請求項１８】　印刷を行う機密情報の印刷権限を確認するため使用される印刷要求データの少なくとも一部を、ドキュメントサーバでのみ復号可能なように暗号化しプリンタ経由で前記ドキュメントサーバに送信する手順をコンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。
【請求項１９】　プリンタ経由でユーザから印刷要求データを受信する受信手順と、
前記印刷要求データに基づくユーザ認証方式がユーザの公開鍵証明書に基づく認証であって、ユーザの公開鍵証明書にはユーザのアクセス権を示すクラス名が記載されており、ドキュメントサーバにおける印刷権限の確認がこのユーザの公開鍵証明書に記載されているクラス名に基づいて行う認証手順をコンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。
【請求項２０】　印刷を行う機密情報の印刷権限を確認するため使用される印刷要求データの少なくとも一部を、ドキュメントサーバでのみ復号可能なように暗号化しプリンタ経由で前記ドキュメントサーバに送信する手順をコンピュータに実行させるためのプログラム。
【請求項２１】　プリンタ経由でユーザから印刷要求データを受信する受信手順と、
前記印刷要求データに基づくユーザ認証方式がユーザの公開鍵証明書に基づく認証であって、ユーザの公開鍵証明書にはユーザのアクセス権を示すクラス名が記載されており、ドキュメントサーバにおける印刷権限の確認がこのユーザの公開鍵証明書に記載されているクラス名に基づいて行う認証手順をコンピュータに実行させるためのプログラム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、ドキュメントサーバ上で管理されている機密性を含むドキュメントを、ネットワークに接続されたプリンタに対して、安全に印刷する技術に関するものである。
【０００２】
【従来の技術】近年、インターネットとＷＥＢ技術の普及によって、ＷＥＢサーバでドキュメントを公開することが広く行われている。企業内などのイントラネットにおいても、同様にＷＥＢサーバを用いてドキュメントの管理・公開が行われており、機密性を含むドキュメントについてもこれと共通した環境での安全な運用が求められている。
【０００３】特定のプロトコルやサーバではなく、一般的にドキュメントサーバ、ネットワークプリンタと、ユーザが印刷を指示するクライアントがネットワークで接続されている形態を考える。
【０００４】これらを用いて、ユーザが印刷を指示し、ドキュメントのデータがネットワークプリンタに送られる経路を考えると図２２（印刷の形態）のような印刷の形態が考えられる。
【０００５】図２２ａのクライアント印刷は、通常ウェブブラウザなどのアプリケーションによってドキュメントを表示・印刷するときの形態である。また、図２２ｂのサーバ印刷は、クライアントからの印刷指示にもとづきサーバ上で印刷のためのプロセスを起動することで印刷を行う形態である。最後に、図２２ｃの参照印刷は、クライアントがネットワークプリンタにドキュメントの所在情報を含む印刷指示を行い、ネットワークプリンタが自らドキュメントサーバにデータを要求して印刷を行う形態である。
【０００６】このようなドキュメントサーバ、ネットワークプリンタ、クライアントによって構成される機密情報印刷システムにおいて、ドキュメントサーバ上に管理されているドキュメントを印刷しようとする場合、上記クライアント印刷の図を例にとると、一般に、図２３（機密情報印刷の危険）のようなセキュリティ上の危険がある。
【０００７】図中、指摘されているものを簡単に説明する。ドキュメントサーバでは、サーバ自体への不正侵入によって、ドキュメントが漏洩したり、破壊・改竄される危険がある。各要素を結ぶ通信路のそれぞれでは、盗聴による漏洩の危険がある。
【０００８】ネットワークプリンタでは、印刷後のドキュメントの盗難やコピーが行われる危険がある。またネットワークプリンタ自体を悪意のソフトウェアによって模倣しドキュメントそのものや印刷イメージをそっくりコピーされる危険がある。また、ネットワークプリンタ自体は本物であっても、物理的なつなぎ替え、もしくはネットワーク経路の操作によって、ＰＣやワークステーションを経由して印刷を行うようにし、その間にデータをコピーしたり改竄が行われる危険もある。
【０００９】さらにドキュメントにアクセスできるユーザをコントロールしていないのは論外であるが、ユーザ情報（パスワードなど）が盗まれたり、ログインしたままのＰＣを使われて、そのユーザの権限でドキュメントが閲覧・印刷されてしまうという危険もある。
【００１０】ドキュメントを管理する立場からは、このクライアント印刷の形態は、印刷が行われるネットワークプリンタとドキュメントサーバとの接触がないため

に、ネットワークプリンタのなりすましがおこなわれていないか確認する手段がないことも問題である。また、この形態では、ドキュメントデータが必ずクライアントのＰＣを経由するため、ＰＣローカルのコピーや途中のＷＥＢプロキシ上のキャッシュデータからの漏洩を防止しづらいことも問題である。

【００１１】これ以外にも、ドキュメントサーバのなりすましによる偽情報の流布や、偽のネットワーク情報（ＤＮＳなど）によるなりすましなど、機密情報の印刷には多数の危険がある。

【００１２】上記の危険のうち、通信路の盗聴、およびドキュメントサーバ（ＷＥＢサーバ）のなりすましについては、暗号通信と認証のミドルウェアである、ＳＳＬ（Ｓｅｃｕｒｅ　Ｓｏｃｋｅｔｓ　Ｌａｙｅｒ：Ｎｅｔｓｃａｐｅ　Ｃｏｍｍｕｎｉｃａｔｉｏｎｓ　Ｃｏｒｐｏｒａｔｉｏｎ，ＵＳＰ　Ｎｏ．５６５７３９０，ｈｔｔｐ：／／ｗｗｗ．ｎｅｔｓｃａｐｅ．ｃｏｍ／ｅｎｇ／ｓｓｌ３／ｄｒａｆｔ３０２．ｔｘｔ）や、ＴＬＳ（Ｔｒａｎｓｐｏｒｔ　Ｌａｙｅｒ　Ｓｅｃｕｒｉｔｙ：ＩＥＴＦ（Ｉｎｔｅｒｎｅｔ　Ｅｎｇｉｎｅｅｒｉｎｇ　ＴａｓｋＦｏｒｃｅ）、ＲＦＣ　２２４６，ｈｔｔｐ：／／ｗｗｗ．ｉｅｔｆ．ｏｒｇ／ｒｆｃ／ｒｆｃ２２４６）を用いることによって、ＷＥＢサーバをＳＳＬ対応とし、ＷＥＢブラウザからの接続時にＷＥＢサーバの認証（オプションでクライアントの認証）と暗号通信を行い、その危険を防止することが広く行われている。

【００１３】これらでも利用されている、より一般的な技術としては、「公開鍵暗号による暗号化と復号」、「デジタル署名」、「公開鍵証明書に基づく認証」および暗号化通信があげられる。むろんこれらは特定のネットワークプロトコルに制約されることはない。これらの技術について、ここで説明することは省くが、（岡本栄司著、暗号理論入門、共立出版株式会社）や、（岡本龍明、山本博資著、現代暗号、産業図書）などに詳しい解説がある。

【００１４】なお、図２３（機密情報印刷の危険）のドキュメントサーバへの不法侵入による盗み見や改鼠および印刷後の盗難の各危険については、システムおよびＯＳ毎の対応やハードウェア的なサポートなどの別種の対応が必要となるので、以下では言及しない。

【００１５】

【発明が解決しようとする課題】上記「従来の技術」にあげた機密情報印刷のセキュリティ上の危険の内、印刷に先立ってネットワークプリンタがなりすまされていないか確認する「プリンタの認証」は通常行われていない。

【００１６】また、プリンタの認証によってなりすましが行われていないことは確認できても、そのネットワークプリンタが当該文書を印刷するのに適したセキュリティ機能を持っていたり、適切な運用が行われているとは限らないので、それらが確認されたプリンタ（以下、安全なプリンタ）だけに印刷データを送るようにしなければならない。

【００１７】また、機密情報印刷のセキュリティ上の危険以外に、前記参照印刷の形態においては、ユーザ認証情報は必ずネットワークプリンタを経由してドキュメントサーバに送られるため、通信路の盗聴やネットワークプリンタのなりすましによってユーザ認証情報を不正に得、これを再使用することによりドキュメントを再取得したり、他のドキュメントのアクセスにこのユーザ認証情報を流用するという危険が存在する。

【００１８】本発明の目的は、上述のように、ネットワークプリンタのなりすましを防止し、安全なプリンタのみへの印刷を可能とすることである。

【００１９】本発明の他の目的は、上記の危険を防止するため、参照印刷の形態において、ネットワークプリンタを経由してドキュメントサーバに送られるユーザ認証情報が他の目的に使用できないようにすることである。

【００２０】

【課題を解決するための手段】本発明の一観点によれば、ネットワークで接続されたドキュメントサーバ、プリンタ、ユーザクライアントから構成される印刷システムであって、プリンタは公開鍵証明書とこれに対応する秘密鍵とを保有し、ドキュメントサーバもしくはユーザクライアントからの要求に応じて公開鍵証明書に基づくプリンタ認証を行うことを特徴とする印刷システムが提供される。

【００２１】本発明の他の観点によれば、公開鍵証明書とこれに対応する秘密鍵とを保有し、外部からの要求に応じて公開鍵証明書に基づくプリンタ認証を行うことを特徴とする印刷装置が提供される。

【００２２】本発明のさらに他の観点によれば、内蔵する機密情報と対応づけられた印刷許可プリンタのリストを保有し、印刷要求が行われた際に出力先のプリンタが前記印刷許可プリンタのリストに含まれるかどうかに応じてドキュメントサーバから送信された印刷データの印刷を行うことを特徴とする印刷装置が提供される。

【００２３】本発明のさらに他の観点によれば、公開鍵証明書とこれに対応する秘密鍵とを保有し、外部からの要求に応じて公開鍵証明書に基づくプリンタ認証を行うステップを有することを特徴とする印刷方法が提供される。

【００２４】本発明のさらに他の観点によれば、内蔵する機密情報と対応づけられた印刷許可プリンタのリストを保有し、印刷要求が行われた際に出力先のプリンタが前記印刷許可プリンタのリストに含まれるかどうかに応じて、前記出力先のプリンタに印刷データを送信するステップを有することを特徴とする印刷方法が提供される。

【００２５】本発明のさらに他の観点によれば、公開鍵証明書とこれに対応する秘密鍵とを保有し、外部からの要求に応じて公開鍵証明書に基づくプリンタ認証を行う手順をコンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体が提供される。

【００２６】本発明のさらに他の観点によれば、内蔵する機密情報と対応づけられた印刷許可プリンタのリストを保有し、印刷要求が行われた際に出力先のプリンタが前記印刷許可プリンタのリストに含まれるかどうかに応じて、前記出力先のプリンタに印刷データを送信する手順をコンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体が提供される。

【００２７】本発明のさらに他の観点によれば、公開鍵証明書とこれに対応する秘密鍵とを保有し、外部からの要求に応じて公開鍵証明書に基づくプリンタ認証を行う手順をコンピュータに実行させるためのプログラムが提供される。

【００２８】本発明のさらに他の観点によれば、内蔵する機密情報と対応づけられた印刷許可プリンタのリストを保有し、印刷要求が行われた際に出力先のプリンタが前記印刷許可プリンタのリストに含まれるかどうかに応じて、前記出力先のプリンタに印刷データを送信する手順をコンピュータに実行させるためのプログラムが提供される。

【００２９】本発明のさらに他の観点によれば、ネットワークで接続されたドキュメントサーバ、プリンタ、ユーザクライアントから構成され、前記プリンタを経由する参照印刷を行う印刷システムであって、印刷を行う機密情報の印刷権限を確認するため使用される印刷要求データの少なくとも一部を、前記ドキュメントサーバでのみ復号可能なように前記ユーザクライアントにおいて暗号化し送付することを特徴とする印刷システムが提供される。

【００３０】本発明のさらに他の観点によれば、印刷を行う機密情報の印刷権限を確認するため使用される印刷要求データの少なくとも一部を、ドキュメントサーバでのみ復号可能なように暗号化しプリンタ経由で前記ドキュメントサーバに送信することを特徴とする印刷装置が提供される。

【００３１】本発明のさらに他の観点によれば、プリンタ経由でユーザから印刷要求データを受信する受信手段と、前記印刷要求データに基づくユーザ認証方式がユーザの公開鍵証明書に基づく認証であって、ユーザの公開鍵証明書にはユーザのアクセス権を示すクラス名が記載されており、ドキュメントサーバにおける印刷権限の確認がこのユーザの公開鍵証明書に記載されているクラス名に基づいて行う認証手段とを有することを特徴とする印刷装置が提供される。

【００３２】本発明のさらに他の観点によれば、印刷を行う機密情報の印刷権限を確認するため使用される印刷要求データの少なくとも一部を、ドキュメントサーバでのみ復号可能なように暗号化しプリンタ経由で前記ドキュメントサーバに送信するステップを有することを特徴とする印刷方法が提供される。

【００３３】本発明のさらに他の観点によれば、プリンタ経由でユーザから印刷要求データを受信する受信ステップと、前記印刷要求データに基づくユーザ認証方式がユーザの公開鍵証明書に基づく認証であって、ユーザの公開鍵証明書にはユーザのアクセス権を示すクラス名が記載されており、ドキュメントサーバにおける印刷権限の確認がこのユーザの公開鍵証明書に記載されているクラス名に基づいて行う認証ステップとを有することを特徴とする印刷方法が提供される。

【００３４】本発明のさらに他の観点によれば、印刷を行う機密情報の印刷権限を確認するため使用される印刷要求データの少なくとも一部を、ドキュメントサーバでのみ復号可能なように暗号化しプリンタ経由で前記ドキュメントサーバに送信する手順をコンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体が提供される。

【００３５】本発明のさらに他の観点によれば、プリンタ経由でユーザから印刷要求データを受信する受信手順と、前記印刷要求データに基づくユーザ認証方式がユーザの公開鍵証明書に基づく認証であって、ユーザの公開鍵証明書にはユーザのアクセス権を示すクラス名が記載されており、ドキュメントサーバにおける印刷権限の確認がこのユーザの公開鍵証明書に記載されているクラス名に基づいて行う認証手順をコンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体が提供される。

【００３６】本発明のさらに他の観点によれば、印刷を行う機密情報の印刷権限を確認するため使用される印刷要求データの少なくとも一部を、ドキュメントサーバでのみ復号可能なように暗号化しプリンタ経由で前記ドキュメントサーバに送信する手順をコンピュータに実行させるためのプログラムが提供される。

【００３７】本発明のさらに他の観点によれば、プリンタ経由でユーザから印刷要求データを受信する受信手順と、前記印刷要求データに基づくユーザ認証方式がユーザの公開鍵証明書に基づく認証であって、ユーザの公開鍵証明書にはユーザのアクセス権を示すクラス名が記載されており、ドキュメントサーバにおける印刷権限の確認がこのユーザの公開鍵証明書に記載されているクラス名に基づいて行う認証手順をコンピュータに実行させるためのプログラムが提供される。

【００３８】本発明によれば、プリンタのなりすましを防止し、安全なプリンタへのみ印刷することができる。また、参照印刷の形態において、プリンタを経由してド

ギュメントサーバに送られるユーザ認証情報が他の目的に使用できないようにすることができる。

【００３９】

【発明の実施の形態】以下、本発明の実施形態を、実施例に沿って図面を参照しながら説明する。

（第１の実施例）図１は本発明における第１の実施例の機密情報印刷システムの構成図の構成図である。

【００４０】図２はサーバ印刷のプロトコル図、図３はドキュメントサーバ上の印刷制御手段の処理のフローチャート、図４はネットワークプリンタのプリンタ制御手段の処理のフローチャートである。

【００４１】図１において、クライアント１１８は、ユーザによって入力された印刷要求データに従って印刷を行なう印刷要求手段１１５と、データの暗号化や復号を行ない、サーバと暗号通信を行なうための暗号通信手段１１４から成る。また、ドキュメントサーバ１１６は、クライアントからの印刷要求を受け取って印刷制御手段に渡す印刷要求受付手段１０８と、クライアントに指定されたプリンタを安全であると確認するために照合する安全なプリンタリスト１０２、印刷を要求するユーザが正当な印刷権限を持っているかを確認するために照合する印刷権限を持つユーザのリスト１０３、サーバの公開鍵証明書とサーバの秘密鍵から成るサーバを認証するためのサーバ認証情報１０４を保有しておく記憶手段１０１と、ドキュメントを保存しておくための記憶装置であるドキュメント保存手段１０６と、プリンタの認証及び安全性の確認やユーザの印刷権限の確認、およびドキュメントデータを取り出し印刷データとして送信するといった一連の作業を行なう印刷制御手段１０５と、クライアントと暗号通信を行なうための暗号通信手段１０９およびプリンタと暗号通信を行なうための暗号通信手段１０７から成る。また、ネットワークプリンタ１１７は、プリンタの公開鍵証明書とプリンタの秘密鍵から成るプリンタを認証するためのプリンタ認証情報を保有する記憶手段１１１と、サーバの認証を行ない、印刷データを受信して出力装置に渡すプリンタ制御手段１１２と、サーバと暗号通信を行なうための暗号通信手段１１０と、印刷データを紙に出力する装置である印刷手段１１３から成る。

【００４２】上述の構成よりなる実施例の動作を、順を追って説明する。本実施例では、前記印刷の形態のうち「サーバ印刷」を例に説明を行なう。

【００４３】ユーザはクライアント１１８の印刷要求手段１１５を用いて、印刷したいドキュメント、出力したいネットワークプリンタ、そのドキュメントの印刷が許可されているユーザを認証するための情報などの印刷要求データを入力する。印刷したいドキュメントやネットワークプリンタは、例えばＷＥＢサーバ上のＵＲＬ（Ｕｎｉｆｏｒｍ　Ｒｅｓｏｕｒｃｅ　Ｌｏｃａｔｏｒ）／ＵＲＩ（Ｕｎｉｆｏｒｍ　Ｒｅｓｏｕｒｃｅ　Ｉｄｅｎｔｉｆｉｅｒ）などの形式で行なう。ユーザ認証のための情報としては、例えばユーザ名とパスワードを使用することもできる。

【００４４】印刷要求手段１１５は、次にこれらの印刷要求データを暗号通信手段１１４およびドキュメントサーバ上の暗号通信手段１０９を経由して、印刷要求受付手段１０８に送る。印刷要求受付手段１０８は、受け取ったデータを印刷制御手段１０５に渡し、印刷のプロセスが開始される。

【００４５】印刷のプロセスの詳細は、図３の印刷制御手段の処理のフローチャートに記されているので、これを参照しながら説明する。

【００４６】印刷制御手段１０５は、受け取った印刷要求データから、ドキュメントを指定する情報（以下、ドキュメントＵＲＩ）とユーザ認証のための情報を抽出する（Ｓ１２０）。

【００４７】次に印刷制御手段１０５は、ユーザ認証情報に基づいてユーザの認証を行い、さらに印刷権限をもつユーザのリスト１０３とユーザ名を照合して、当該ドキュメントの印刷権があるか確認する（Ｓ１２１）。ユーザ認証が失敗しているか、印刷権がないと判断（Ｓ１２２のｎｏ）された場合には、印刷拒否の通知をクライアント１１８に行なって（Ｓ１２９）、処理は終了する。ユーザ認証と印刷権が確認（Ｓ１２２ｙｅｓ）された場合は、印刷制御手段１０５は、印刷要求データから指定された印刷先のネットワークプリンタのＵＲＩを取り出し、安全なプリンタのリスト１０２と照合する（Ｓ１２３）。

【００４８】指定されたネットワークプリンタが当該ドキュメントを出力してよいリストに含まれていない場合（Ｓ１２４のｎｏ）、印刷拒否の通知をクライアント１１８に行なって（Ｓ１３０）処理は終了する。指定されたネットワークプリンタが当該ドキュメントを出力してよいリストに含まれている場合（Ｓ１２４のｙｅｓ）は、次のプリンタの認証に移る。

【００４９】本実施例では、プリンタの認証は単独に行なうものではなく、サーバ認証といっしょに行なう形で書かれているが、サーバのなりすましの排除を行わない場合は、サーバ認証を省略した形で行なうこともできる。

【００５０】サーバ・プリンタの相互認証は、ドキュメントサーバの暗号通信手段１０７とネットワークプリンタの暗号通信手段１１０を経由して、サーバ認証情報１０４とプリンタ認証情報１１１を用いた公開鍵証明書に基づく認証を相互に行なうことで実施する。この詳細については、従来の技術にあげた参考文献を参照されたい。

【００５１】また、上記の説明で、暗号通信手段１１４，１０９，１０７，１１０については特に指定しなかったが、従来の技術のＳＳＬやＴＬＳを使用してＴＣＰ

／ＩＰによる通信を行なう場合、ＳＳＬ／ＴＬＳでは暗号通信を行なう前にサーバ認証を（オプションとしてクライアント（この場合だとネットワークプリンタ）認証）行なうことができるので、印刷制御手段１０５での処理を省略することも可能である。

【００５２】さて、サーバ・プリンタの相互認証が成功しなかった場合（Ｓ１２６のｎｏ）、印刷制御手段１０５は印刷拒否の通知をクライアントに行なって（Ｓ１３１）処理を終了する。サーバ・プリンタの相互認証が成功した場合（Ｓ１２６のｙｅｓ）には、ネットワークプリンタに印刷データを送信し（Ｓ１２７）、正常終了の通知を行なう（Ｓ１２８）。

【００５３】印刷データは、ドキュメントサーバ１１６上の暗号化通信手段１０７からネットワークプリンタ１１７上の暗号化通信手段１１０を経由してプリンタ制御手段１１２に渡される。

【００５４】ネットワークプリンタにおける出力までのプロセスの詳細は、図４のプリンタ制御手段処理のフローチャートに記されているので、これを参照しながら説明する。

【００５５】ネットワークプリンタでは、前記したようにドキュメントサーバからの印刷データ受信に先立ってサーバ・プリンタ相互認証を行なっている（Ｓ１４０）。次にドキュメントサーバから認証結果を受信し（Ｓ１４１）、認証が失敗（Ｓ１４２のｎｏ）すればそのまま処理を終了する。認証が成功（Ｓ１４２のｙｅｓ）すれば、プリンタ制御手段１１２は、印刷データを受信し（Ｓ１４３）、印刷手段１１３に印刷データを渡す。印刷手段１１３は印刷を実行し（Ｓ１４４）、印刷終了後に印刷終了通知（Ｓ１４５）を行なって処理を終了する。

【００５６】以上のクライアント、ドキュメントサーバ、ネットワークプリンタの相互の通信プロトコルを図２に示し、以下手順を追って説明を行なう。

【００５７】まず、クライアントはドキュメントサーバに対してサーバ認証を行なう。サーバ認証が成功したならば、クライアントはユーザによって入力されたドキュメントＵＲＩ、プリンタＵＲＩ、ユーザ認証情報を印刷要求データとしてドキュメントサーバに印刷要求する。ドキュメントサーバでは、受信したユーザ認証情報に基づくユーザ認証を行ない、ユーザ認証が失敗（ＮＧ）したならば、印刷拒否通知（応答（ＮＧ））をクライアントに送って、処理を終了する。

【００５８】ユーザ認証が成功（ＯＫ）したならば、ドキュメントサーバとネットワークプリンタ間で相互認証を行ない、認証が失敗（ＮＧ）したならば、ドキュメントサーバからクライアントに印刷拒否通知が送られて処理を終了する。認証が成功（ＯＫ）すれば、ドキュメントサーバはネットワークプリンタに印刷要求を行ない、ネットワークプリンタは印刷を受け付けたことをドキュメントサーバに返す。続いて、ドキュメントサーバはネットワークプリンタに印刷データを送信し、ネットワークプリンタは受信した印刷データを印刷する。印刷が終了したら、ネットワークプリンタは、ドキュメントサーバに印刷終了通知を行ない、処理を終了する。ドキュメントサーバは、印刷終了通知を受信したら、クライアントに対して印刷完了通知（応答（成功））を行ない、処理を終了する。

【００５９】以上のように、ネットワークプリンタの公開鍵証明書に基づく認証と、安全なプリンタとして登録されているリストとの照合とを行えば、不適格なプリンタへの出力が避けられる。

【００６０】なお、図３の印刷制御手段のフローチャートで、安全なプリンタリストとの照合（Ｓ１２３，Ｓ１２４）とプリンタ認証（Ｓ１２５，Ｓ１２６）は逆の順序で行っても支障ない。

【００６１】（第２の実施例）上記第１の実施例では、ドキュメントサーバが安全なプリンタのリストを持つことによりプリンタの安全性の確認を行なう方式を説明したが、本実施例では、プリンタ認証に使用する公開鍵証明書の拡張部（ｅｘｔｅｎｓｉｏｎ）にプリンタの安全性のクラスを示す情報が記載されているものとし、これを使用してプリンタの安全性を確認する方式について説明する。

【００６２】安全性のクラスを示す情報としては、例えば、ネットワークプリンタがＩＣカードなどのカード読み取り器を有し、印刷した本人の身分証明用ＩＣカードを挿入しないと印刷物を取り出せないような機構を備えている場合に、メーカが公開し、安全性を保証しているプリンタのクラス名称として、Ｓｅｃｕｒｉｔｙ－Ｃｌａｓｓ：“ＣｌａｓｓＡ－Ｐｒｉｎｔｅｒ”とする場合などがこれにあたる。図７にこの例を図示する。また、同様に印刷後のデータをプリンタから消し去ってしまい、分解してハードディスク装置などをアクセスしてもデータを盗むことが困難であることをメーカが保証するクラス名などもこのようなクラスを示す情報として利用できる。

【００６３】図５は本発明における第２の実施例の機密情報印刷システムの構成図である。図６はこの構成におけるドキュメントサーバにおける印刷制御手段の処理のフローチャートである。

【００６４】図５の機密情報印刷システムの構成図において、図１と同番号の要素は図１と同内容であるので説明を省略する。ドキュメントサーバ２１６において、記憶手段１０１に保有する情報が、安全なプリンタリスト１０２ではなく安全とみなすクラスのリスト２０１になっている。また、ネットワークプリンタ２１７の記憶手段に保有するプリンタ認証拡張情報２０３は、前記のようにプリンタの公開鍵証明書拡張部（ｅｘｔｅｎｓｉｏｎ）にプリンタの安全性のクラスを示す情報を追加した

プリンタの公開鍵証明書とこれと対応する秘密鍵から成るものである。

【００６５】以下、第１の実施例と異なる部分を中心に、本実施例における処理を図６の印刷制御手段の処理のフローチャートを参照しながら説明する。

【００６６】図６の印刷制御手段の処理のフローチャートにおいて、開始から印刷権限を持つユーザのリストと照合し、印刷権限を確認する（Ｓ１２１，Ｓ１２２）までは、図１と同じ処理である。

【００６７】その後、サーバ・プリンタ相互認証をし（Ｓ１２５）、認証が成功しなかった場合（Ｓ１２６のｎｏ）、印刷制御手段２０２は、印刷拒否の通知をクライアントに行なって（Ｓ１３１）処理を終了する。

【００６８】認証が成功した場合（Ｓ１２６のｙｅｓ）には、サーバ・プリンタ相互認証の際に得られたプリンタ認証拡張情報２０３のプリンタの公開鍵証明書からｅｘｔｅｎｓｉｏｎを取り出し、ここに記述されている情報（クラス）を、安全とみなすクラスのリスト２０１と照合する（Ｓ２２５）。指定されたネットワークプリンタが当該ドキュメントを出力してよいリストに含まれていない場合（Ｓ２２６のｎｏ）、印刷拒否の通知をクライアントに行なって（Ｓ１３０）、処理を終了する。指定されたネットワークプリンタが当該ドキュメントを出力してよいリストに含まれている場合（Ｓ２２６ｙｅｓ）は、ネットワークプリンタに印刷データを送信し（Ｓ１２７）、正常終了の通知を行なう（Ｓ１２８）。

【００６９】ネットワークプリンタにおける出力までのプロセスの詳細は、実施例１における図４のプリンタ制御手段の処理のフローチャートと同じであり、また、クライアント、ドキュメントサーバ、ネットワークプリンタの相互の通信プロトコルは図２と同じであるため、ここでの説明は省略する。

【００７０】以上のように、ネットワークプリンタの公開鍵証明書に基づく認証と、公開鍵証明書のｅｘｔｅｎｓｉｏｎに記述されている安全性のクラスを示す情報を用いて安全とみなすプリンタのクラスのリストとの照合とを行なえば、不適格なプリンタへの出力が避けられ、さらに、同じクラスに属するプリンタの記述は１つで済むため、安全とみなすプリンタのリストを使用する場合と比較して、プリンタの追加や削除といった手間を省くことができる。

【００７１】（第３の実施例）本実施例では、第１の実施例と同様に、サーバが安全なプリンタリストを持ち、プリンタ認証後に、安全なプリンタであるか否かをリストと照合して確認する方式を、参照印刷の形態について説明する。

【００７２】図８は本発明における第３の実施例の機密情報印刷システムの構成図である。図９は参照印刷のプロトコル図、図１０，図１１はこの構成におけるプリンタのプリンタ制御手段の処理のフローチャート、図１２はこの構成におけるサーバの印刷データ制御手段の処理のフローチャートである。

【００７３】図８の機密情報印刷システムの構成図において、図１と同番号の要素は図１と同内容であるので説明を省略する。

【００７４】ドキュメントサーバ３１６の印刷制御手段３０１の処理と、ネットワークプリンタ３１７のプリンタ制御手段３０２の処理と、クライアント３１８の印刷要求手段の処理の内容については後で詳しく説明する。

【００７５】上述の構成よりなる実施例の動作を、順を追って詳細に説明する。クライアント３１８は印刷要求手段３０５を用いて、ユーザによって要求された印刷したいドキュメント、出力したいネットワークプリンタ、そのユーザによって入力されたドキュメントの印刷が許可されているユーザを認証するための情報などから印刷要求データを生成する。印刷したいドキュメントやネットワークプリンタは、例えばＷＥＢサーバ上のＵＲＬ／ＵＲＩなどの形式で行なう。

【００７６】ユーザ認証のための情報としては、例えばユーザ名とパスワードを使用することもできる。印刷要求手段３０５は、次にこれらの印刷要求データを暗号通信手段３０４およびネットワークプリンタ３１７の暗号通信手段３０３を経由して、プリンタ制御手段３０２に送る。

【００７７】このプリンタ制御手段３０２におけるクライアント・プリンタ間の処理は図１０のクライアント・プリンタ間の処理（ａ）に記されているので、これを参照しながら説明する。

【００７８】初めにクライアントとネットワークプリンタ間でプリンタ認証を行なう。プリンタの認証は、クライアント３１８の暗号通信手段３０４とネットワークプリンタ３１７の暗号通信手段３０３を経由して行ない。プリンタ認証情報１１１を用いた公開鍵証明書に基づく認証を行なうことで実施する。

【００７９】ネットワークプリンタは、プリンタ認証情報１１１をクライアントに送信し（Ｓ３４０）、クライアントから認証結果を受信する（Ｓ３４１）。認証が失敗（Ｓ３４２のｎｏ）ならばそのまま処理を終了する。認証が成功（Ｓ３４２のｙｅｓ）したならばクライアントから印刷要求データを受信（Ｓ３４３）して、サーバ・プリンタ間の処理（Ａ）に移る。

【００８０】次にプリンタ制御手段３０２は、受け取った印刷要求データを暗号通信手段１１０およびドキュメントサーバ上の暗号通信手段１０７を経由してドキュメントサーバ３１６の印刷データ制御手段３０１に送り、印刷データを要求する。

【００８１】このプリンタ制御手段３０２におけるプリンタ・サーバ間の処理は図１１のプリンタ・サーバ間の処理（ｂ）に記されているので、これを参照しながら説明する。

【００８２】まず、ネットワークプリンタとドキュメントサーバ間においてプリンタ認証を行なう（Ｓ３４４，Ｓ３４５）。

【００８３】本実施例では、プリンタの認証は単独に行なうものではなく、サーバ認証といっしょに行なう形で書かれているが、サーバのなりすましの排除を行なわない場合は、サーバ認証を省略した形で行なうこともできる。

【００８４】サーバ・プリンタの相互認証は、ドキュメントサーバ３１６の暗号通信手段１０７とネットワークプリンタ３１７の暗号通信手段１１０を経由して、サーバ認証情報１０４とプリンタ認証情報１１１を用いた公開鍵証明書に基づく認証を相互に行なうことで実施する。この詳細については、従来の技術にあげた参考文献を参照されたい。

【００８５】また、上記の説明で、暗号通信手段１０７，１１０，３０３，３０４については特に指定しなかったが、公知技術のＳＳＬやＴＬＳを使用してＴＣＰ／ＩＰによる通信を行なう場合、ＳＳＬ／ＴＬＳでは暗号通信を行なう前にサーバ認証（この場合クライアントのプリンタ認証ではネットワークプリンタ、プリンタ・サーバ相互認証ではドキュメントサーバ）を、オプションとしてクライアント（この場合だとネットワークプリンタ）認証を行なうことができるので、プリンタ制御手段３０２及び印刷データ制御手段３０１での処理を省略することも可能である。

【００８６】さて、ネットワークプリンタは、サーバ・プリンタの相互認証が成功しなかった場合（Ｓ３４６のｎｏ）、処理を終了する。サーバ・プリンタの相互認証が成功した場合（Ｓ３４６のｙｅｓ）には、ドキュメントサーバに印刷要求データを送ることで印刷データを要求する（Ｓ３４７）。次にドキュメントサーバからユーザ認証結果を受信し（Ｓ３４８）、ユーザ認証が成功しなかった場合（Ｓ３４９のｎｏ）、処理を終了する。ユーザ認証が成功した場合（Ｓ３４９のｙｅｓ）には、印刷データを受信し（Ｓ３５０）、印刷データを印刷手段１１３に渡す（Ｓ３５１）。印刷が終了したらネットワークプリンタは、クライアントに印刷終了を通知して（Ｓ３５２）、処理を終了する。

【００８７】また、印刷データ制御手段３０１におけるプロセスは、図１２の印刷データ制御手段の処理のフローチャートに記されているので、これを参照しながら説明する。

【００８８】ドキュメントサーバは、ネットワークプリンタから印刷データを要求されたら、前記のサーバ・プリンタ相互認証を行なう（Ｓ３２０）。サーバ・プリンタの相互認証が成功しなかった場合（Ｓ３２１のｎｏ）、印刷データ制御手段３０１は印刷拒否の通知をプリンタ経由でクライアントに行なって（Ｓ３２９）、処理を終了する。サーバ・プリンタの相互認証が成功した場合（Ｓ３２１のｙｅｓ）には、印刷データ制御手段３０１は、印刷要求データから印刷先のネットワークプリンタのＵＲＩを取り出し、安全なプリンタのリスト１０２と照合する（Ｓ３２２）。ネットワークプリンタが当該ドキュメントを出力してよいリストに含まれていない場合（Ｓ３２３のｎｏ）、印刷拒否の通知をプリンタ経由でクライアントに行なって（Ｓ３３０）、処理を終了する。ネットワークプリンタが当該ドキュメントを出力してよいリストに含まれている場合（Ｓ３２３のｙｅｓ）は、印刷データ制御手段３０１は、受け取った印刷要求データから、ドキュメントＵＲＩとユーザ認証情報を抽出する（Ｓ３２４）。次に印刷データ制御手段３０１は、ユーザ認証情報に基づいてユーザの認証を行ない、さらに印刷権限をもつユーザのリスト１０３とユーザ名を照合して、当該ドキュメントの印刷権があるか確認する（Ｓ３２５）。ユーザ認証が失敗しているか、印刷権がないと判断（Ｓ３２６のｎｏ）された場合には、印刷拒否の通知をプリンタ経由でクライアントに行なって（Ｓ３３１）、処理を終了する。ユーザ認証と印刷権が確認（Ｓ３２６のｙｅｓ）された場合は、ネットワークプリンタに印刷データを送信し（Ｓ３２７）、正常終了の通知を行ない（Ｓ３２８）、処理を終了する。

【００８９】以上のクライアント、ドキュメントサーバ、ネットワークプリンタの相互の通信プロトコルを図９に示し、以下手順を追って説明を行なう。

【００９０】まず、クライアントはネットワークプリンタに対してプリンタ認証を行なう。プリンタ認証が成功したならば、クライアントはドキュメントＵＲＩとユーザによって入力されたユーザ認証情報を印刷要求データとしてネットワークプリンタに送信する。ネットワークプリンタとドキュメントサーバ間で相互認証を行ない、認証が失敗（ＮＧ）したならば、クライアントに印刷拒否通知が送られて処理を終了する。認証が成功（ＯＫ）すれば、ネットワークプリンタはドキュメントサーバに印刷データを要求する。ドキュメントサーバでは、受信したユーザ認証情報に基づくユーザ認証を行ない、ユーザ認証が失敗（ＮＧ）したならば、印刷拒否通知（応答（ＮＧ））をプリンタ経由でクライアントに通知して、処理を終了する。ユーザ認証が成功（ＯＫ）したならば、ドキュメントサーバはネットワークプリンタに印刷データを送信する。ネットワークプリンタは受信した印刷データを印刷し、印刷が終了したならば、クライアントに印刷完了通知（応答（成功））を行ない、処理を終了する。

【００９１】以上のように、ネットワークプリンタの公開鍵証明書に基づく認証と、安全なプリンタとして登録されているリストとの照合とを行なえば、不適格なプリンタへの出力が避けられる。

【００９２】（第４の実施例）本実施例では、参照印刷の形態で起こりうるユーザ認証情報の盗用への対策を説

明する。

【００９３】図１３は本発明の第４の実施例の機密情報印刷システムの構成図である。図中、ドキュメントサーバ５１６中の印刷データ制御手段５０１は、図８の参照印刷形態の実施例３の印刷データ制御手段の処理内容を変更したものである。変更された処理内容は図１５の印刷データ制御手段の処理のフローチャートに記載されている。

【００９４】また、クライアント５１８中の印刷要求データ暗号化手段５０２と印刷要求手段５０３は本実施例に特有の処理を行っており、その処理内容については後述する。

【００９５】ドキュメントサーバ５１６中の１０１，１０２，１０３，１０４，１０６，１０７、およびネットワークプリンタ５１７中の１１０，１１１，１１３は図１の同番号要素と、また、ネットワークプリンタ５１７中の３０２，３０３およびクライアント５１８中の３０４は図８の同番号要素と同じものであるので、説明を省略する。

【００９６】次に上述の構成よりなる実施例の動作を、実施例３との差異を中心に詳述する。前述のように、参照印刷の形態においては、ユーザ認証情報は必ずネットワークプリンタを経由してドキュメントサーバに送られることから、通信路の盗聴やネットワークプリンタのなりすましによって得たユーザ認証情報を再使用することによるドキュメントの再取得や、他のドキュメントのアクセスへのユーザ認証情報の流用という危険が存在する。

【００９７】これに対応するため、本実施例のクライアント５１８は印刷要求手段５０３を用いて印刷要求データを生成する際に、印刷要求データ暗号化手段５０２を用いて印刷要求データの少なくとも一部をドキュメントサーバのみが復号できるように暗号化する。

【００９８】この暗号化の方法としては、ドキュメントサーバの公開鍵証明書に含まれる公開鍵（事前に入手しておくか、この時点でドキュメントサーバと前記のＳＳＬ／ＴＬＳなどで接続すれば入手可能）を使用した暗号化があげられる。公開鍵暗号の性質として広く知られていることであるが、これは、特定の公開鍵で暗号化されたデータは、その公開鍵と対応する秘密鍵でのみ復号できるという性質を利用したものであり、ドキュメントサーバの公開鍵で暗号化したデータは、ドキュメントサーバのみが保有している秘密鍵のみで復号できる。

【００９９】暗号化する印刷要求データとしては、ユーザ認証の方式がユーザ名・パスワードであれば、少なくともパスワードを暗号化すべきであるが、その他にも、他のドキュメントのアクセスにこの印刷要求データが流用されるのを防止するためにドキュメントＵＲＩを含めたり、他のネットワークプリンタからの利用を防止するためにプリンタＵＲＩを含めることが有効である。

【０１００】また、なりすましたネットワークプリンタが同一の印刷要求データを何度も利用して複数の印刷を行うことを防止するには、印刷要求データを生成した時刻データやシリアルナンバー、乱数など、特定の印刷要求データを他と識別できるデータを添付して暗号化することも有効である。暗号化した印刷データの例を図１６に示す。

【０１０１】さて、印刷要求手段５０３によって生成された印刷要求データはネットワークプリンタ５１７を経由してドキュメントサーバ５１６に送られるが、ネットワークプリンタ５１７上の処理は、実施例３の図１１のステップＳ３４７の印刷データ要求の際に送付する印刷要求データの一部が暗号化されているのみで、その処理内容に変化はない。図１４の参照印刷のプロトコル（５）に、暗号化したユーザ認証情報が送られる様子を示す。

【０１０２】次にドキュメントサーバ５１６における処理を、図１５の印刷データ制御手段の処理のフローチャートを参照しつつ説明する。図１５と実施例３の図１２との差異は、Ｓ５２４（図１２ではＳ３２４）のステップで、クライアント５１８で少なくとも一部が暗号化された印刷要求データを、サーバ認証情報１０４の一部としてドキュメントサーバのみが保有しているドキュメントサーバの秘密鍵を用いて復号した後、必要なデータを抽出する部分のみである。

【０１０３】なおこの際、印刷要求データに上で述べたドキュメントＵＲＩやプリンタＵＲＩ、印刷要求生成時刻などが含まれている場合は、印刷データを要求してきたプリンタとプリンタＵＲＩの比較を行ったり、印刷要求されたドキュメントとドキュメントＵＲＩとを比較することによって、印刷要求データの盗用・流用を防止することができる。また印刷要求データ生成時刻から特定の短い時間の間だけ、印刷要求データが有効であるような制御をドキュメントサーバで行ったり、特定の印刷要求データを識別するのに使用できる印刷要求生成時刻やシリアルナンバーのようなデータを用いれば、なりすましたネットワークプリンタが同じ印刷要求データを複数回使用することも防止可能となる。

【０１０４】以上、説明したように、本実施例によれば、参照印刷の形態で起こりうるユーザ認証情報の盗用もしくは再利用を防止することができ、ネットワークプリンタの認証および安全なプリンタの確認とあいまって、当該ドキュメントを印刷する権限のある正当なユーザにだけ、安全なプリンタへの印刷を可能とすることができる。

【０１０５】（第５の実施例）本実施例では、参照印刷の形態で起こりうるユーザ認証情報の盗用への対策として、ユーザの公開鍵証明書を使用する方法について説明する。

【０１０６】図１７は本発明の第５の実施例の機密情報

印刷システムの構成図である。図中、ドキュメントサーバ６１６中の印刷データ制御手段６０２は、図１３の参照印刷形態の実施例４の印刷データ制御手段５０１の処理内容を変更したものである。変更された処理内容は図１９の印刷データ制御手段の処理のフローチャートに記載されている。

【０１０７】また印刷権限を持つクラスのリスト６０１は、図１３の印刷権限を持つユーザのリスト１０３に代わるものである。この内容および使用方法は後述する。

【０１０８】また、クライアント６１８中の記憶手段６０５に格納されているユーザ認証拡張情報６０３、および印刷要求手段６０４は本実施例に特有の処理を行っており、その内容および処理内容については後述する。また、印刷要求データ暗号化手段５０２は図１３の同番号要素と同一のものである。

【０１０９】ドキュメントサーバ６１６中の１０１，１０２，１０４，１０６，１０７、およびネットワークプリンタ６１７中の１１０，１１１，１１３は図１の同番号要素と、また、ネットワークプリンタ６１７中の３０２，３０３およびクライアント６１８中の３０４は図８の同番号要素と同じものであるので、説明を省略する。

【０１１０】次に上述の構成よりなる実施例の動作を、実施例４との差異を中心に詳述する。実施例４では、ユーザ認証方式がユーザ名・パスワードである例について説明を行ったが、本実施例ではユーザの公開鍵証明書に基づくユーザ認証方式を採用している場合について説明する。

【０１１１】クライアント６１８の印刷要求手段６０４は、印刷すべきドキュメントＵＲＩや印刷先のネットワークプリンタＵＲＩなどの印刷要求データの入力を受けたあと、これら印刷要求データの一部もしくは全部、またはそれらのダイジェスト情報に対して、ユーザ認証拡張情報６０３に含まれる公開鍵証明書に対応した秘密鍵を使って、デジタル署名を生成する。（このデジタル署名は、後にドキュメントサーバ６１６上で印刷要求に含まれる印刷要求データを確認する際、これらが改竄されていないことの証明となる。）クライアント６１８の印刷要求手段６０４は、このデジタル署名を添付した印刷要求データを新たな印刷要求データとし、実施例４と同様に印刷要求データ暗号化手段５０２を用いてドキュメントサーバの公開鍵で暗号化して、ネットワークプリンタ６１７を経由してドキュメントサーバ６１６に送る。

【０１１２】なおドキュメントサーバのユーザ認証がＬＤＡＰなどのディレクトリサービスを用いて行われておらず、ユーザの公開鍵証明書が入手できない場合は、上記印刷要求データにデジタル署名とともに、ユーザの公開鍵証明書自体を添付してやればよい。印刷要求データとデジタル署名の例を図２０に示す。

【０１１３】ネットワークプリンタ６１７上の処理は、実施例４と同様に（実施例４でも参照した、実施例３の図１１のステップＳ３４７の）印刷データを要求する際に送付する、印刷要求データの形式が実施例４と異なるのみで、その処理内容に変化はない。図１８の参照印刷のプロトコル（６）に、暗号化したユーザ認証拡張情報が送られる様子を示す。

【０１１４】ネットワークプリンタ６１７を経由して、印刷要求を受け取ったドキュメントサーバ６１６は、印刷データ制御手段６０２を用いて処理を行う。図１９の印刷データ制御手段の処理のフローチャートがその内容であるが、この内容は実施例４の印刷データ制御手段５０１の処理内容とは、Ｓ６２２のユーザ認証と分岐Ｓ６２３と認証失敗による印刷拒否通知Ｓ６３１、およびＳ６２４，Ｓ６２５からなる印刷権限の確認部分で異なっている。

【０１１５】まずＳ６２２でユーザ認証を行う。ユーザ認証はユーザのデジタル署名の正しさを確認することで行われる。サーバの公開鍵で復号された印刷要求データからドキュメントＵＲＩやプリンタＵＲＩなど、クライアント６１８の印刷要求手段６０４で生成したデジタル署名の対象であるデータを抽出し（ダイジェスト情報を使用している場合は、これらのダイジェスト情報を作成して）、同じく復号された印刷要求データから抽出されたデジタル署名とこれが対応しているか否かをユーザの公開鍵を用いて確認する（Ｓ６２２）。

【０１１６】ここでユーザの公開鍵は、ドキュメントサーバのユーザ認証がＬＤＡＰなどのディレクトリサービスを用いて行われていればそこから、そうでない場合は、上記印刷要求データにデジタル署名とともに添付されているユーザの公開鍵証明書から抽出して使用すればよい。デジタル署名と対象データの対応が取れず、認証が失敗した場合（Ｓ６２３のｎｏ）は印刷拒否通知（認証失敗）Ｓ６３１を行い、処理は終了する。認証が成功した場合（Ｓ６２３のｙｅｓ）は、Ｓ６２４，Ｓ６２５のドキュメントの印刷権限の確認に移る。

【０１１７】実施例４ではドキュメントの印刷権限の確認はドキュメントと関連付けられた印刷権限を持つユーザのリストとの照合であったが、本実施例ではユーザの公開鍵証明書の拡張部に記された特定のユーザのクラスを使用する方法を用いている。ここで、クライアント６１８のユーザ認証拡張情報６０３に含まれるユーザの公開鍵証明書の拡張部にはドキュメントのアクセス権にかかわるクラス名が記入されているものとし、これがドキュメントに関連付けられた印刷を許可されたクラスのリスト６０１を満たす場合、印刷権ありとなる。アクセス権にかかわるクラス名としてはたとえば職制や職務上の担当などがあげられる。

【０１１８】図２１にユーザの所属組織などが発行した拡張部付きのユーザの公開鍵証明書の例を示すが、この例ではユーザの職制が部長クラスであることを示しており、ドキュメントサーバ上で部長以上の印刷を許可する

機密情報についてユーザ認証成功となる。

【０１１９】ステップＳ６２４では、印刷要求データの一部として送られてきたユーザの公開鍵証明書の拡張部を抽出し、ユーザのアクセス権にかかわるクラス名を得る。次にＳ６２５は、ドキュメントサーバ６１６の印刷権限を持つクラスのリスト６０１とこの情報とを照合し、印刷権限を確認する。以降の処理は実施例４と同じである。

【０１２０】本方法の利点としては、ユーザ名そのものではなく、ユーザのクラスに対して印刷権限が設定されるため、ドキュメントに関連付けられた印刷を許可されたクラスのリストの管理の手間が小さくなることがあげられる。

【０１２１】以上説明したように、本実施例によれば、ドキュメントサーバの公開鍵による印刷要求データの暗号化に加え、ユーザの公開鍵証明書を用いた認証とデジタル署名により、印刷要求データが偽造あるいは流用される危険性をさらに小さくすることができ、参照印刷の形態で起こりうるユーザ認証情報の盗用もしくは再利用を防止することができる。また、ネットワークプリンタの認証および安全なプリンタの確認とあいまって、当該ドキュメントを印刷する権限のある正当なユーザにだけ、安全なプリンタへの印刷を可能とすることができる。

【０１２２】なお、クライアント６１８の印刷要求手段６０４は、デジタル署名を添付した印刷要求データを、印刷要求データ暗号化手段５０２を用いてドキュメントサーバの公開鍵で暗号化して送っているが、実施例４とは異なり、本実施例では印刷要求データにはデジタル署名がなされていることから偽造は困難であると考えられる。従って、なりすましたネットワークプリンタが印刷要求データを復号できないことは必ずしも必要ではなく、クライアントにおける印刷要求データのドキュメントサーバの公開鍵による暗号化と、ドキュメントサーバにおける復号の処理は省略することも可能である。

【０１２３】また、実施例４および実施例５で示した印刷要求データ（あるいはユーザ認証情報）の盗用もしくは再利用を防止する手法は、実施例２で示した安全なプリンタの確認に、ドキュメントに対応した安全クラスを使用する方法と組み合わせることも可能であり、これらの組み合わせによっても、当該ドキュメントを印刷する権限のある正当なユーザにのみ、安全なプリンタへの印刷を可能とするという目的を達成することができる。

【０１２４】以上の通り、印刷に先立って、当該ネットワークプリンタの認証を行い、正当性が確認されたプリンタについて、そのドキュメントの印刷許可があるかどうかの確認を行う必要がある。このためには、ネットワークプリンタ内にそのプリンタを特定できる公開鍵証明書とこれに対応する秘密鍵を持たせ、ドキュメントデータの送信に先立って、公開鍵証明書に基づくプリンタの認証を行う。さらに、ドキュメントサーバ上に、ドキュメントの適切な分類と対応した安全なネットワークプリンタのリストを持たせ、これと認証したネットワークプリンタとの照合を行う。以上により、上記課題が解決できる。

【０１２５】ドキュメントデータの送信に先立って、ネットワークプリンタの公開鍵証明書に基づく認証と、ドキュメントの適切な分類と対応したプリンタの安全性の確認を行なうことにより、ネットワークプリンタのなりすましを防止し、安全なプリンタのみへの印刷を可能とすることができる。

【０１２６】また、ユーザクライアントはユーザ認証情報を含む印刷要求データの少なくとも一部を、ドキュメントサーバのみが復号可能なように暗号化して送る。しかる後に、ネットワークプリンタを経由して、一部を暗号化した印刷要求データを受け取ったドキュメントサーバが、当該ドキュメントのユーザの印刷権限の確認を行う際、印刷要求の偽造が行われていないことを確認することにより、ユーザ認証情報や印刷を指示する情報が盗用され、ドキュメントの再取得や他のドキュメントのアクセスに流用されることを防止することができる。

【０１２７】ドキュメントサーバ上で管理されている機密性を含むドキュメントを、ネットワークに接続されたプリンタに印刷するシステムにおいて、参照印刷の形態で起こりうるユーザ認証情報の盗用もしくは再利用を防止することができ、ネットワークプリンタの認証および安全なプリンタの確認とあいまって、当該ドキュメントを印刷する権限のある正当なユーザにだけ、安全なプリンタへの印刷を可能とすることができる。

【０１２８】本実施例は、コンピュータがプログラムを実行することによって実現することができる。また、プログラムをコンピュータに供給するための手段、例えばかかるプログラムを記録したＣＤ－ＲＯＭ等の記録媒体又はかかるプログラムを伝送するインターネット等の伝送媒体も本発明の実施例として適用することができる。上記のプログラム、記録媒体及び伝送媒体は、本発明の範疇に含まれる。

【０１２９】なお、上記実施例は、何れも本発明を実施するにあたっての具体化のほんの一例を示したものに過ぎず、これらによって本発明の技術的範囲が限定的に解釈されてはならないものである。すなわち、本発明はその技術思想、またはその主要な特徴から逸脱することなく、様々な形で実施することができる。

【０１３０】

【発明の効果】以上説明したように本発明によれば、プリンタのなりすましを防止し、安全なプリンタへのみ印刷することができる。また、参照印刷の形態において、プリンタを経由してドキュメントサーバに送られるユーザ認証情報が他の目的に使用できないようにすることができる。

【図面の簡単な説明】

【図１】本発明の実施例１による機密情報印刷システムの構成図である。

【図２】サーバ印刷のプロトコルを示す図である。

【図３】実施例１における印刷制御手段の処理を説明するフローチャートである。

【図４】実施例１におけるプリンタ制御手段の処理を説明するフローチャートである。

【図５】本発明の実施例２による機密情報印刷システムの構成図である。

【図６】実施例２における印刷制御手段の処理を説明するフローチャートである。

【図７】拡張されたプリンタの公開鍵証明書を示す図である。

【図８】本発明の実施例３による機密情報印刷システムの構成図である。

【図９】参照印刷のプロトコルを示す図である。

【図１０】実施例３におけるプリンタ制御手段の処理を説明するフローチャートである。

【図１１】実施例３におけるプリンタ制御手段の処理を説明するフローチャートである。

【図１２】実施例３における印刷データ制御手段の処理を説明するフローチャートである。

【図１３】本発明の実施例４による機密情報印刷システムの構成図である。

【図１４】参照印刷のプロトコルを示す図である。

【図１５】実施例４における印刷データ制御手段の処理を説明するフローチャートである。

【図１６】実施例４におけるクライアントが生成する印刷要求データを説明する図である。

【図１７】本発明の実施例５による機密情報印刷システムの構成図である。

【図１８】参照印刷のプロトコルを示す図である。

【図１９】実施例５における印刷データ制御手段の処理を説明するフローチャートである。

【図２０】実施例５におけるユーザの公開鍵証明書を用いる場合の印刷要求データを説明する図である。

【図２１】拡張部付きのユーザの公開鍵証明書を示す図である。

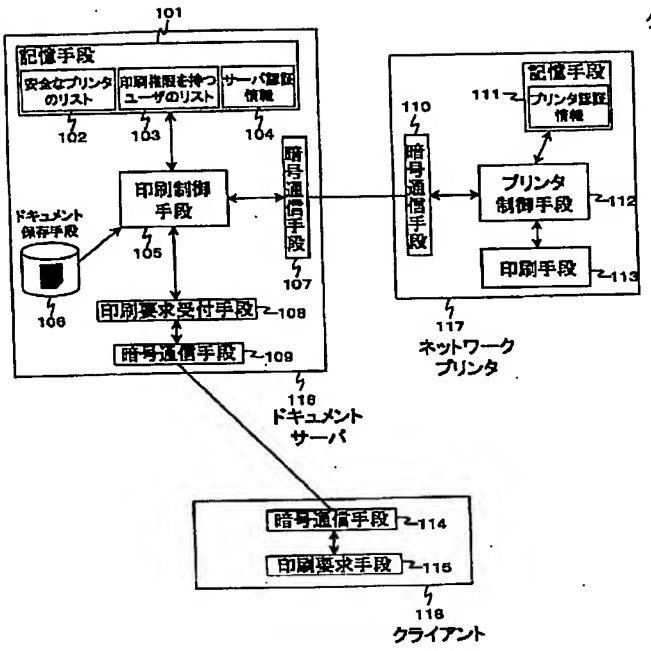
【図２２】印刷の形態を示す図である。

【図２３】機密情報印刷の危険性を示す図である。

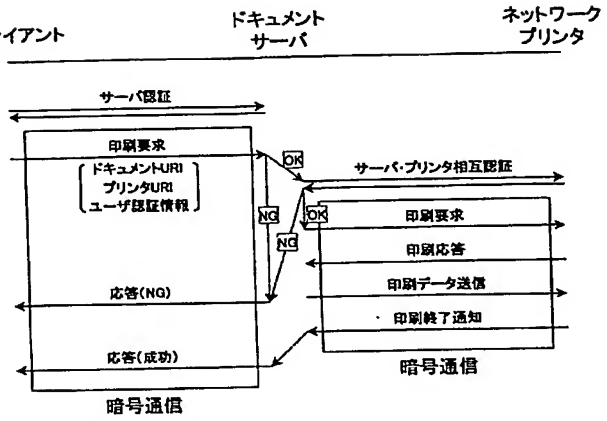
【符号の説明】

１０１　記憶手段
１０３　印刷権限を持つユーザのリスト
１０５　印刷制御手段（サーバ印刷）
１０７　暗号通信手段
１０９　暗号通信手段
１１１　記憶手段
１１３　印刷手段
１１５　印刷要求手段（サーバ印刷）
１１７　ネットワークプリンタ
２０１　安全とみなすクラスのリスト
２０３　プリンタ認証拡張情報
２１７　ネットワークプリンタ
３０１　印刷データ制御手段
３０３　暗号通信手段
３０５　印刷要求手段（参照印刷）
３１７　ネットワークプリンタ
５０１　印刷データ制御手段
５０３　印刷要求手段（参照印刷）
５１７　ネットワークプリンタ
６０１　印刷権限を持つクラスのリスト
６０３　ユーザ認証拡張情報
６０５　記憶手段
６１７　ネットワークプリンタ
１０２　安全なプリンクリスト
１０４　サーバ認証情報
１０６　ドキュメント保存手段
１０８　印刷要求受付手段
１１０　暗号通信手段
１１２　プリンタ制御手段（サーバ印刷）
１１４　暗号通信手段
１１６　ドキュメントサーバ
１１８　クライアント
２０２　印刷制御手段
２１６　ドキュメントサーバ
２１８　クライアント
３０２　プリンタ制御手段（参照印刷）
３０４　暗号通信手段
３１６　ドキュメントサーバ
３１８　クライアント
５０２　印刷要求データ暗号化手段
５１６　ドキュメントサーバ
５１８　クライアント
６０２　印刷データ制御手段
６０４　印刷要求手段（参照印刷）
６１６　ドキュメントサーバ
６１８　クライアント

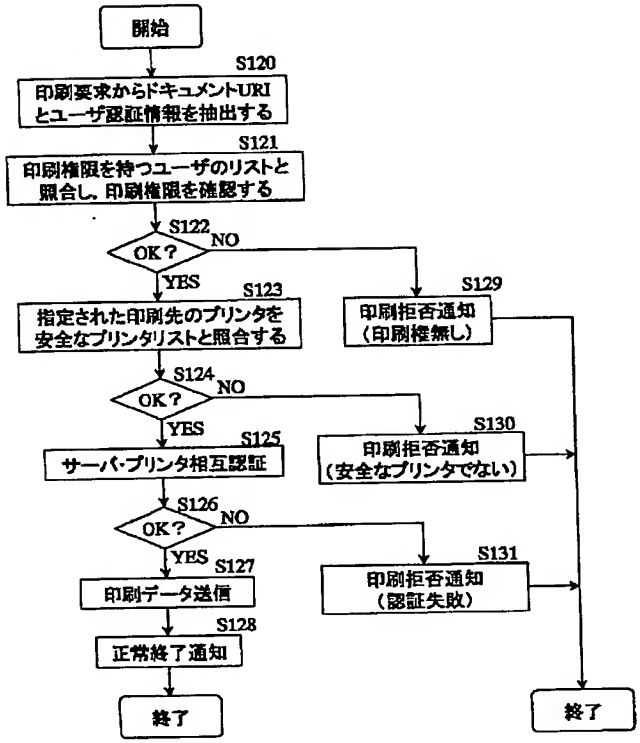
【図１】


101
記憶手段
安全なプリンタのリスト
印刷権限を持つユーザのリスト
サーバ認証情報
102
103
104
印刷制御手段
暗号通信手段
107
ドキュメント保存手段
106
105
印刷要求受付手段
108
暗号通信手段
109
116
ドキュメントサーバ
記憶手段
111
プリンタ認証情報
110
暗号通信手段
プリンタ制御手段
112
印刷手段
113
117
ネットワークプリンタ
暗号通信手段
114
印刷要求手段
115
118
クライアント

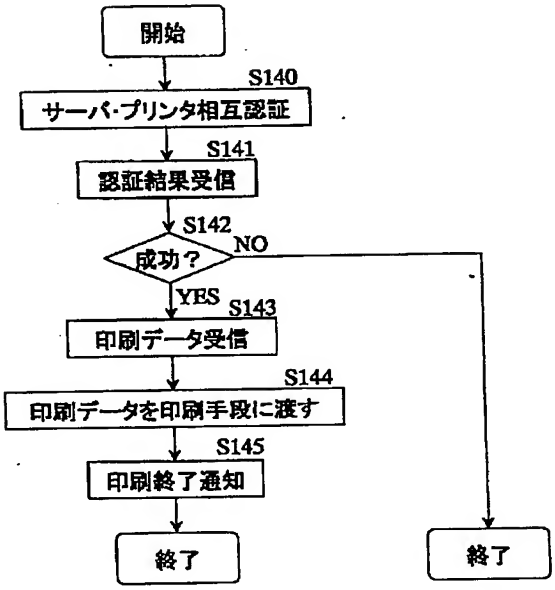
【図２】


クライアント
ドキュメントサーバ
ネットワークプリンタ
サーバ認証
印刷要求
ドキュメントURI
プリンタURI
ユーザ認証情報
OK
NG
NG
サーバ・プリンタ相互認証
OK
印刷要求
印刷応答
印刷データ送信
印刷終了通知
応答(NG)
応答(成功)
暗号通信
暗号通信

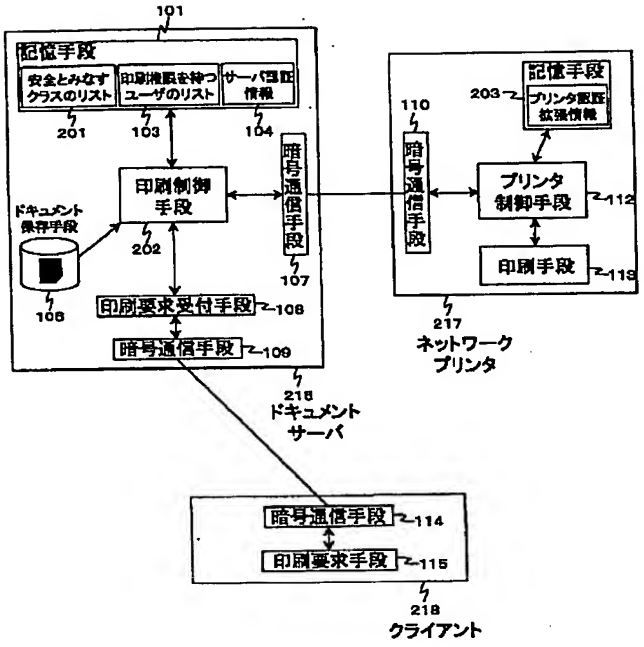
【図３】


開始
S120
印刷要求からドキュメントURIとユーザ認証情報を抽出する
S121
印刷権限を持つユーザのリストと照合し、印刷権限を確認する
S122
OK？
NO
YES
S123
指定された印刷先のプリンタを安全なプリンタリストと照合する
S129
印刷拒否通知（印刷権無し）
S124
OK？
NO
YES
S125
サーバ・プリンタ相互認証
S130
印刷拒否通知（安全なプリンタでない）
S126
OK？
NO
YES
S127
印刷データ送信
S131
印刷拒否通知（認証失敗）
S128
正常終了通知
終了
終了

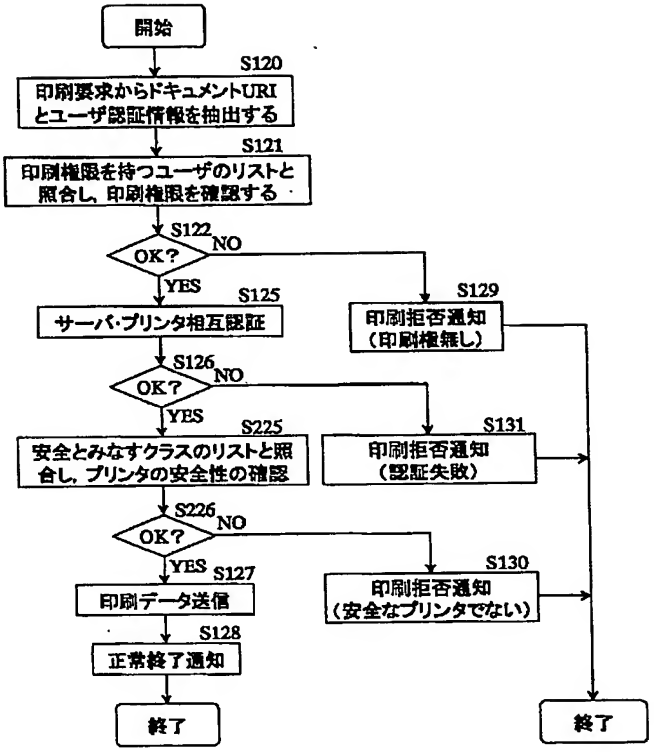
【図４】


開始
S140
サーバ・プリンタ相互認証
S141
認証結果受信
S142
成功？
NO
YES
S143
印刷データ受信
S144
印刷データを印刷手段に渡す
S145
印刷終了通知
終了
終了

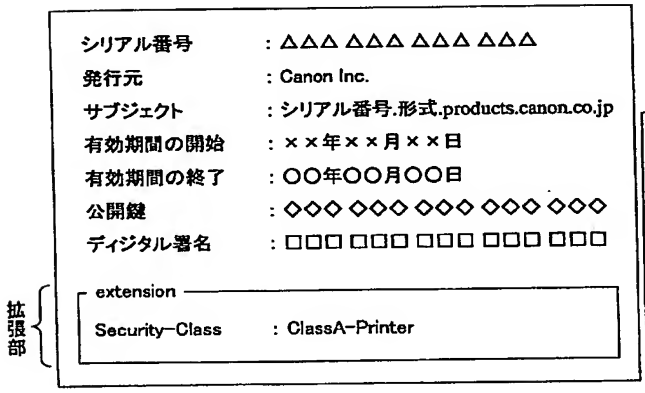
【図５】



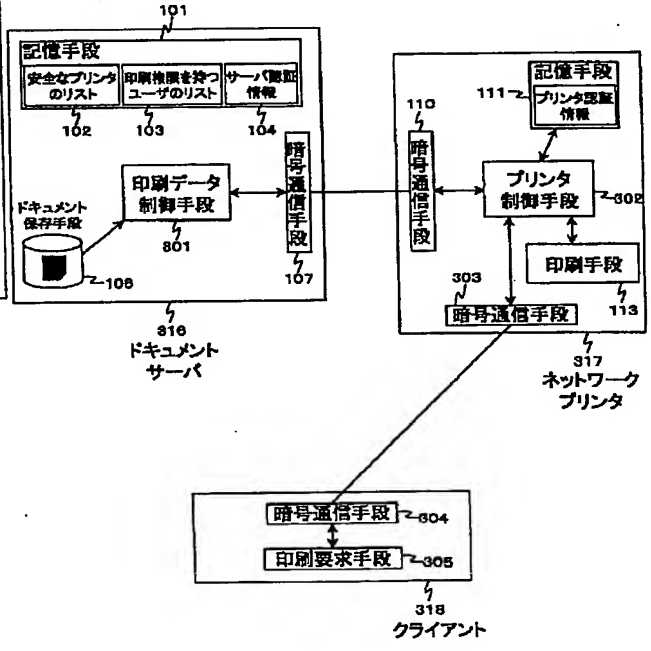
【図６】



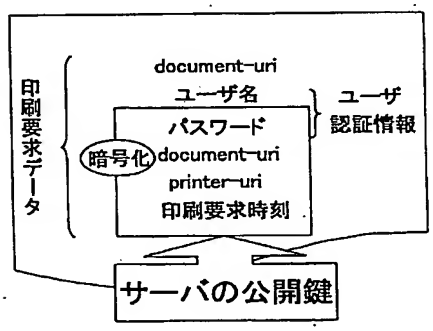
【図７】



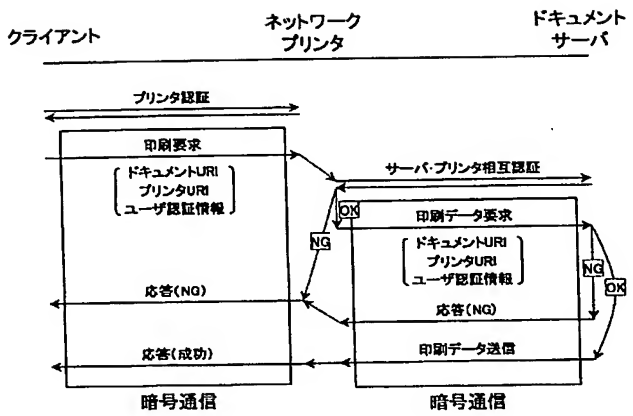
【図８】



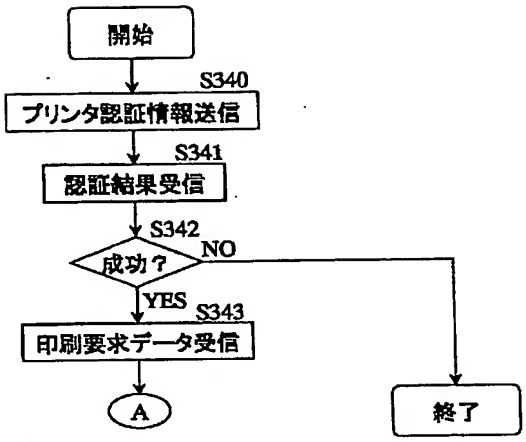
【図１６】



【図９】

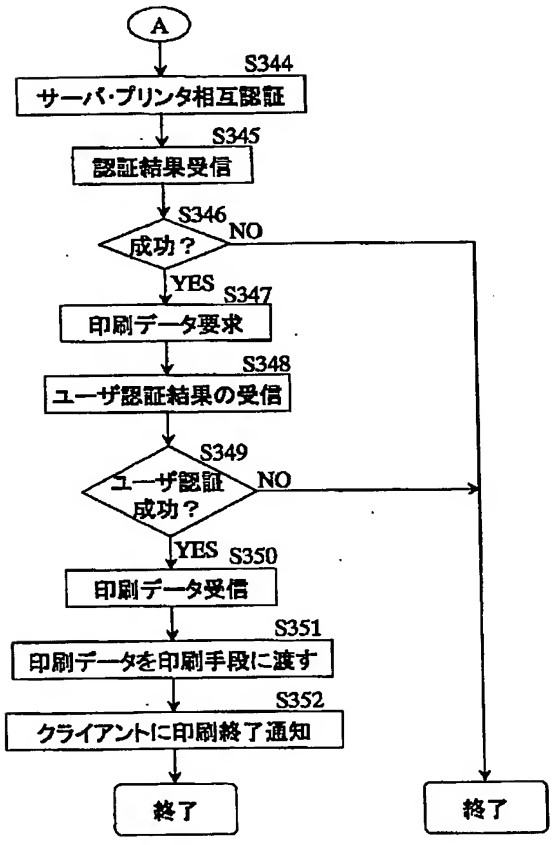


【図１０】

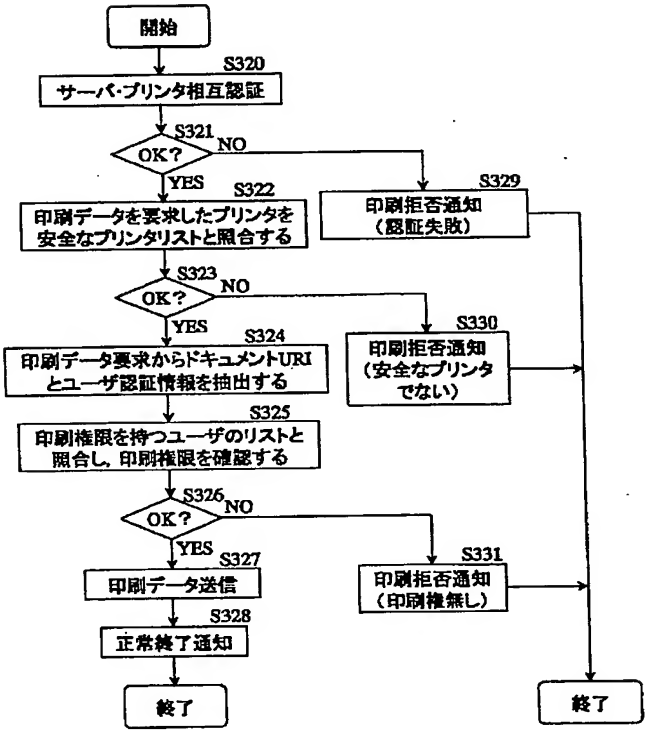


クライアント・プリンタ間の処理

【図１１】

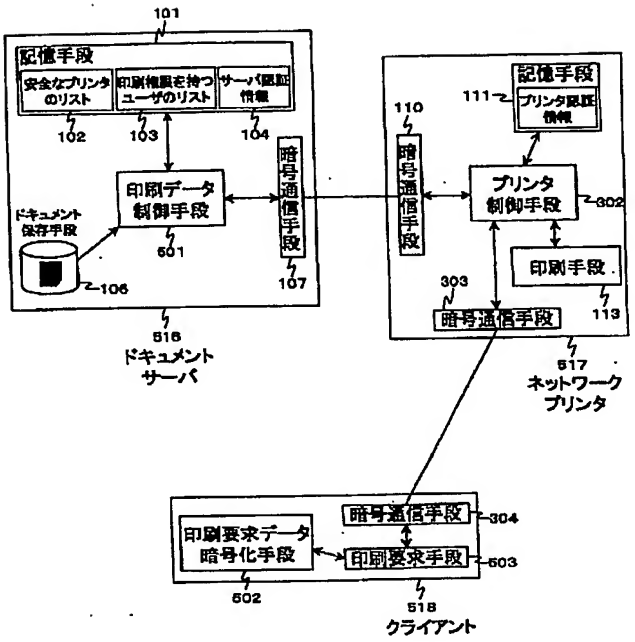


【図１２】

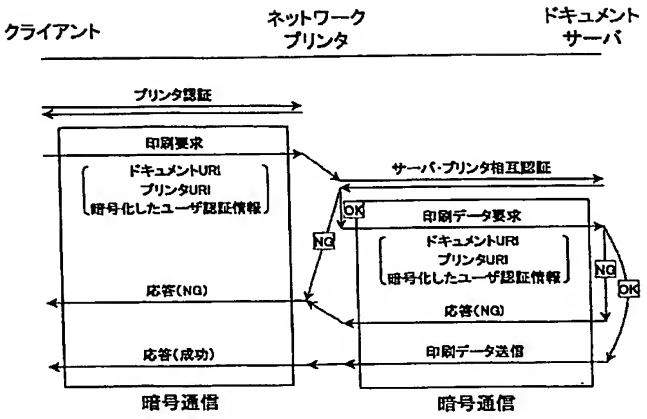


プリンタ・サーバ間の処理

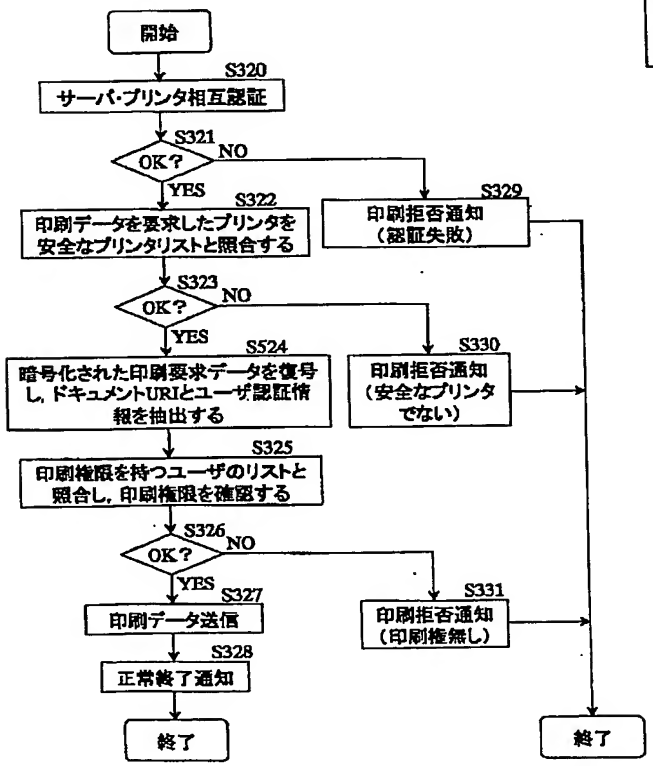
【図１３】



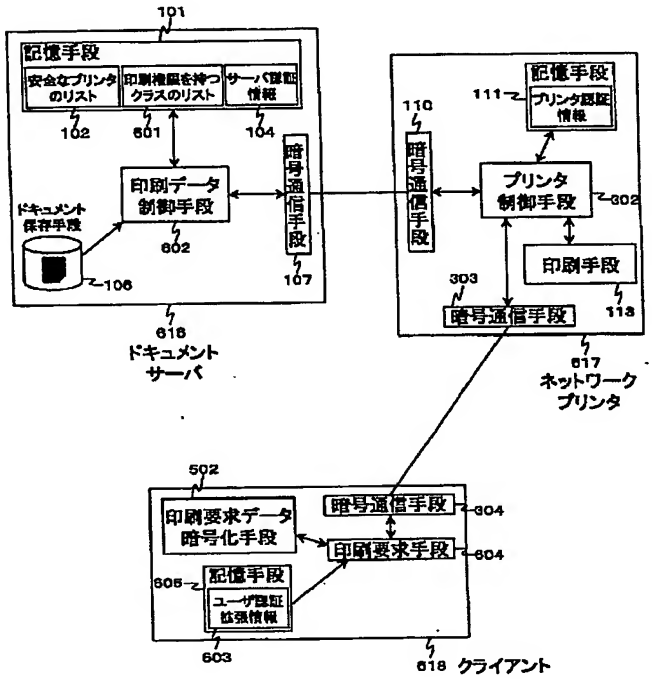
【図１４】



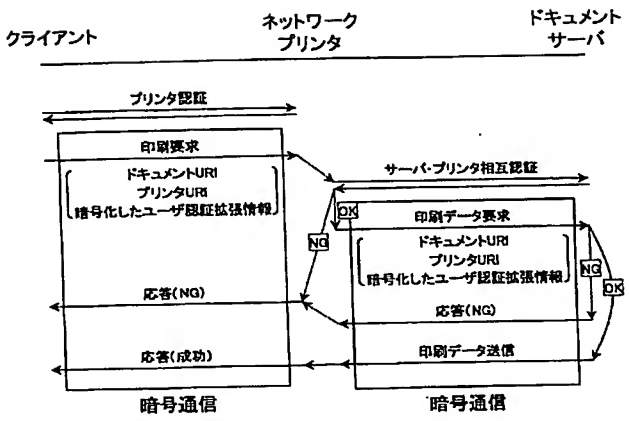
【図１５】



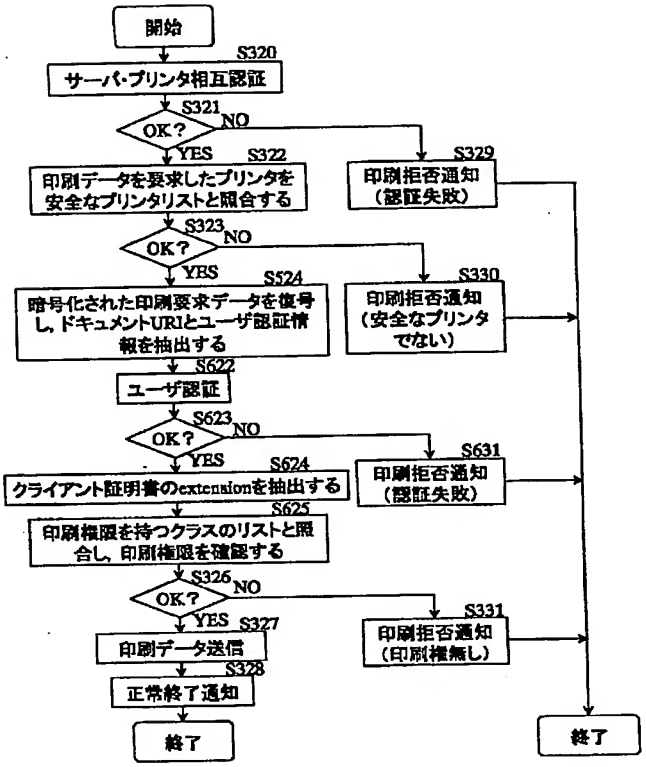
【図１７】



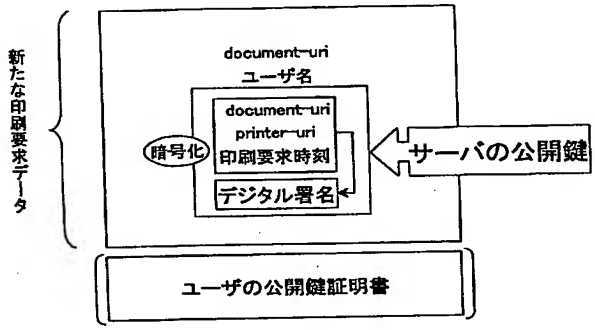
【図１８】



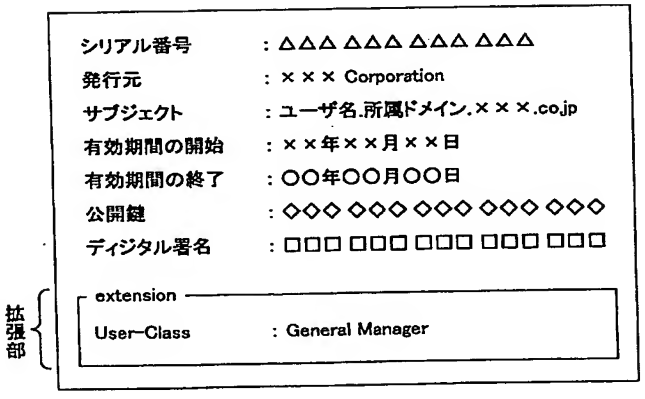
【図１９】



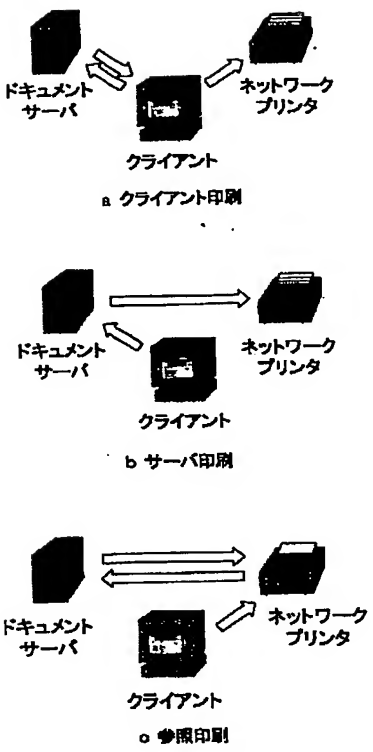
【図２０】



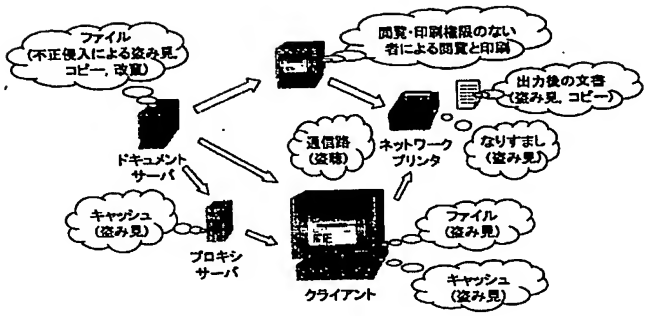
【図２１】



【図２２】



【図２３】



フロントページの続き

Ｆターム(参考)　2C061 AP01 CL08 CL10 HH01 HJ08
HN23 HV01 HV32 HV44 HX10
5B021 AA01 EE02 EE04 NN18
5B085 AA08 AE02 AE03 AE04
5J104 AA07 KA01 KA05 NA02 PA07